REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification): Managing the Double Edged Sword of Network Centric Warfare. (UNCLASSIFIED)

9. Personal Authors: Major David P. Wells, USMC

10.Type of Report: FINAL

11. Date of Report: 30 Jan 2003

12.Page Count: 23

12A Paper Advisor (if any): Professor Thomas G. Mahnken

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: Network-Centric Warfare, NCW, Information Management, IM, JTF, Operational Planning, Operational Art, Operational Level of War

15.Abstract: Network Centric Warfare can tend to collapse the operational level war by allowing information to flow around or past hierarchical staff structures and directly between tactical and strategic level decision makers. Why this has benefits in that it may streamline decision-making and reduce staff sizes, it can have serious detrimental impacts on joint warfare. Fortunately, by employing developed Information Management techniques during planning disciplined staffs can develop methods that will enhance the positive benefits of Network Centric Warfare while negating many of its serious drawbacks and weaknesses.

16.Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

NAVAL WAR COLLEGE
Newport, R.I.

MANAGING THE DOUBLE EDGE SWORD OF NETWORK-CENTRIC WARFARE

by

David P. Wells
Major, USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

30 January 2003

Advisor: Professor Thomas G. Mahnken
Strategy Department

Introduction

Over the past several years there has been a rapid, Department of Defense (DoD) wide migration towards information exchange via state of the art information technologies. Specifically, more and more command, control and coordination functions are being moved onto computer networks that interconnect commanders, staffs and operators from the strategic to the tactical level. In part, this technological transformation is rooted in a concept known as Network-Centric Warfare (NCW) in which the existence of a strong telecommunications network plays a key role. While the pursuit of advanced technology to improve effective combat power is always desirable, there is the hazard of pursuing it too quickly, thereby turning a technological superiority into a critical vulnerability. In the case of NCW as it is being pursued today, the reliance on vast networks of computers and the widespread sharing of a Common Operational Picture (COP) can tend to collapse the operational level of war by allowing information to flow around or past hierarchical staff structures and directly between tactical and strategic level decision makers. While this has benefits in that it may streamline decision-making and optimize staffs, it can have detrimental impacts on joint warfare ranging from information overload to micromanagement. Fortunately, by employing developed Information Management techniques during planning, disciplined staffs can develop methods that will enhance the positive benefits of NCW while negating many of its drawbacks. This paper will briefly describe NCW and how it tends to compress the operational level of war. It will then discuss the current pitfalls of network dependence and the threats that the compression of the operational level of war poses to a Joint Task Force's mission. Finally, it will propose a set of guidelines that builds on Information Management (IM) doctrine that a staff can use to capitalize on the strengths of NCW while avoiding the pitfalls as they exist today.

What Is Network-Centric Warfare?

In the words of Vice Admiral Arthur K. Cebrowski (Ret), the current Director of the Office of Force Transformation within the office of the Secretary of Defense: "Network-Centric Warfare is a concept. As a concept, it cannot have a definition, because concepts and definitions are enemies."[1] Though this lack of definition leaves something to be desired, there fortunately has been much written on models that describe the functioning of the NCW concept and on the desired end-state of a transformation toward it. Individual services and staffs have done even more work on NCW while taking their first steps on the dash down the road towards the fruition of the concept. As described by Adm. Cebrowski, the key components to the NCW are "information superiority, shared awareness, adaptability, speed of command and self synchronization".[2] These NCW components are achieved by the interconnection of widely dispersed commanders, sensors, weapons and operators via integrated telecommunications networks that allow all of these entities to see what needs to be seen and exchange what needs to be exchanged. This information exchange is to happen so quickly that our forces can overwhelm the enemy to such a great extent that, in the best case, he has no viable options against us. This best case scenario puts the enemy in a state of "strategic lockout"[3] where he is always one or more steps behind and is constantly at a disadvantage. Though a fighting force does not necessarily have to achieve lockout for NCW to give it an advantage over its enemy, it is the quintessential end-state to be pursued. NCW proponents have derived this concept of lockout from business models from companies like Sony which locked in its own success with the cost and performance advantages of VHS videotape while locking out the competing Beta standard.[4]

---

[1] Arthur K. Cebrowski, “Network Centric Warfare: An Emerging Military Response to the Information Age,” Lecture, U.S. Naval War College, Newport, RI: Jun 1999, 1.
[2] Ibid., 2.
[3] Alberts, David S., et.al. Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP. 1999. p 156.
[4] Arthur K. Cebrowski and John J. Garstka, “Network Centric Warfare: Its Origins and Future,” U.S. Naval Institute Proceedings. (July 1998): 29

The object of NCW is for a widely distributed fighting force to be able to autonomously attack myriad enemy critical vulnerabilities while individual activities remain in concert with one another, in synchronization with the commander's intent (which can be changing over time), in an environment where sensors, shooters and decision makers are not in proximity to each other but yet are still mutually supporting. This ability to have disparate and geographically distributed assets mutually supporting one another in defeating the enemy in depth across the battlespace is known as "self-synchronization." A common business model for describing the phenomena of self-synchronization is Wal-Mart which shares inventory control information in near real time with its suppliers using network technology. A sale of an item off Wal-Mart's shelf automatically initiates a purchase requisition with the supplier to replace the item without the need for an intermediating central purchasing department.[5] Applied to combat such self-synchronization could imply what is commonly referred to as "just in time logistics" and perhaps very rapid sensor to shooter engagement cycles. Such response is in accordance with the current U.S. Air Force Chief of Staff's call for sensor to shooter response time in single digit minutes.[6] The intent is to mass effects on the enemy without necessarily massing forces.[7] Additionally, it is desirable to maintain initiative and momentum by minimizing operational pauses between actions against the enemy making the attacks more fluid over time. Ideally, if the attacks were near continuous, coordinated in time and distributed over the entirety of the enemy area it would be as if he were being attacked by a "swarm" of heavily armed and deadly bees.[8]

One of models for NCW involves an interaction between resource grids. The first grid, the "sensor grid", contains all of the sensors in a three dimensional battlespace, another grid, the "engagement grid", contains all of the weapons in the battlespace. The third grid, the "Command and Control (C2) or

---

[5] Ibid., 30.
[6] Glen W. Goodman, Jr. "More than Just Platforms & Sensors: US Air Force Pushes Integration of its ISR Assets" The ISR Journal, (2002/Issue 1): 26.
[7] Cebrowski and Garstka, 32.

Information Grid", contains all of the combat decision makers and the information technology that ties them together. These grids overlap within the same battlespace with nodes that are interlinked to provide the right information to the right nodes at the right time to be able to achieve the five components of NCM discussed above.[9] Though information is shared across the battlespace, it is important to note that under the concept of NCW, this does not necessarily mean that all nodes are connected to all others or that all users must have access to the same degree of information or same levels of service.[10] In fact, excessive access to information is one of the key weaknesses in many of today's developing NCW efforts.

Operational Swiss Cheese

Due to its very nature, NCW can tend to collapse the operational level of war or poke holes through it like a block of Swiss cheese. This section will discuss the tendency and some of its pros and cons. By its very nature, NCW has three fundamental effects on the operational level of war, it: 1) eliminates middlemen in decision making processes, 2) enables distance command and coordination, and 3) empowers the force with information.

NCW tends to eliminate middlemen in decision making processes because it allows individuals at all levels of war to be more directly connected. For example, a written order between any two participants in the network can go straight from one commander's keyboard via e-mail to another commander's computer screen at a push of a button. In the past, such a record message would have been drafted, staffed, released, transmitted, received and posted passing through several hands and distributed based on a rule set partly determined by the sender and partly based on a rule set determined by the recipient. The new way of doing business via e-mail or chat rooms eliminates all sorts of the middlemen, the message

---

[8] Edward A. Smith, Jr. "Network-Centric Warfare: What's the Point?", Naval War College Review (Winter 2001): 60, 67.
[9] Repeated from above, the five components are: "Information Superiority, Shared Awareness, Adaptability, Speed of Command and Self Synchronization"
[10] Alberts, Garstka and Stein, 114.

handlers. Although it seldom happens, if these message handlers were clerks who could be converted to trigger pullers, this could be a decidedly good thing. However, when the message handlers eliminated are staff officers who need to act in support of the action ordered but were cut out of the decision loop, there is potential for operational breakdown. In a briefing developed by Admiral James O. Ellis, CJTF NOBLE ANVIL during Operation ALLIED FORCE, he describes how guidance from video teleconferences was prone to misinterpretation as it was "filtered down to lower staff levels".[11] This type of problem is inherent to any point to point communications that are not controlled by some sort of guidelines for publication and distribution. While flattening an organization to increase efficiency is admirable, eliminating too many middlemen in the decision cycle may have the unintended adverse affect of eliminating duty experts as well. To illustrate, Wal-Mart's point of sale inventory control and reordering system discussed above might not work as well if each of the stores picked up and displaced 10 km. every day and there were not a logistics planning staff available to coordinate all of the deliveries. However, this is exactly the situation in warfare as units move about the battlefield, so every hole poked in the operational staff planning may have unexpected second order effects. According to Marine Corps Doctrinal Publication (MCDP) 6:

"We believe that the object of technology is not to reduce the role of people in the command and control process, but rather to enhance their performance -- although technology should allow us to decrease the *number* [emphasis in original] of people involved in the process…. Technology should seek to automate routine functions which machines can accomplish more efficiently than people in order to free people to focus on the aspects of command and control which require *judgment and intuition* [my emphasis]. "[12]

Warfare is a human interaction in which each side has a host of subject matter experts and mission area specialists each trying to anticipate how their opponent will react to their actions.[13] Commanders who

---

[11] Admiral James O. Ellis. "A View from the Top", 21. n.d.
[12] U.S. Marine Corps. MCDP-6 Command and Control, (Washington, DC: 4 Oct 1996): 136.
[13] LtGen Paul K. Van Riper, "Information Superiority" U.S Congress, House, Procurement Subcommittee and Research and Development Subcommittee, 20 March 1997, 6.

bypass these staff experts too often may be penny wise with respect to time but pound foolish with respect to operational success.

In addition to the way that NCW tends to eliminate middlemen, the information technology that enables NCW allows for participants to coordinate over greater and greater distances. The obvious upshot of this is the savings in travel time and expense. Commanders can now coordinate face to face via video teleconference gaining more of the non-verbal communication insight that is missing from voice and text based communications. Some NCW advocates have even gone so far as to suggest using split base operations with bases separated by continents. An example would be a Joint Forces Air Component Commander (JFACC) split between CONUS and a distant theater of operation. Notable benefits to this sort of distance coordination include the savings in airlift and the increased survivability of the rear area fraction of the split JFACC. Drawbacks range from the potential for micromanagement from the rear to the problems of leadership from afar. The most important drawback however, is the potential for a failure of the reach-back communications that allowed the staffs to be split in the first place.[14] How well the command functions when the split staffs are disconnected from one another will be the true measure of effectiveness for this notional command structure.

The third effect of NCW on the operational level of war is that of information empowerment. NCW has been described as "empowering all the decision makers in the battlespace rather than just a few." Since knowledge or, better yet, understanding of a situation is generally a good thing, empowering decision makers generally seems beneficial as long as the decision makers are not burdened with information that is irrelevant or useless to their situation or future operations. If too great, such excess information could result in information overload.[15]

---

[14] Scott M. Britten, "Directing the War from Home," The Technological Arsenal: Emerging Defense Capabilities, (Washington, DC: Smithsonian Institute Press 2001), 210.
[15] Alberts, Garstka and Stein, 104.

Along with the intended benefits of information empowerment come some interesting drawbacks described by Richard Harknett as "micro-management" and "macro-management."[16] Micro-management occurs when high level commanders reach down to control actions too far below their level. Adm. Ellis experienced this phenomena in Kosovo and described it as enabling "senior leadership to sink to past comfort levels …", he further warned that, "… discipline is required to remain at the appropriate level of engagement and command".[17] Micro-management can have adverse impacts on leadership, morale and can cause senior commanders to make low level decisions based on fragmented information and only a partial view as to what is going on below. Macro-management is a phenomena caused by lower echelons knowing too much. Harknett describes this as a "god's-eye view" that may tempt low level commanders to make decisions that should be left to those well above their pay-grade. Tactical actions taken based on this extraneous knowledge could conceivably have severe adverse operational or strategic repercussions. He also poses an interesting question as to what a tactical unit might do if they were fully aware that they were "outnumbered, surrounded, and without hope of timely support to hold their positions". Hopefully, they would do the right thing and complete the mission but they will certainly have a lot more to think about than they ever had to before.[18]

A final drawback to information empowerment is that it can tend to lead to the perpetual pursuit of more information. As Adm. Ellis put it in reference to information technology: "uncontrolled it will control you and your staffs … and lengthen your decision cycle times". This is obviously not our desired outcome for NCW. He also asks the question: "The demand for info will always exceed the capability to

[16] Richard J. Harknett. "The Risks of a Networked Military," Orbis. (Winter 2000): 135.
[17] Ellis, 21.
[18] Harknett, 135.

provide it … how much is enough?"[19] Ultimate knowledge is a tempting apple but we might just learn enough to know that we are wearing no clothes.

The NCW Minefield of Today

Since the United States is just beginning down the path towards the vision of NCW, there are many obstacles and hazards to our success. It is vital that these hazards do not cause our technological advantages to become critical vulnerabilities. Some of these hazards are internal vulnerabilities that we have taken on by decisions made in the implementation of some of our first steps toward NCW. These internal hazards include several technological, operational planning, and human factor or leadership issues. Our potential adversaries will likely have similar internal hazards as they implement network technology into their operations. A second category of hazards is based on burdens that we bare based on being a democratic nation and superpower that are more unique to us and all of our potential adversaries may not share.

The first technological landmine that we armed for ourselves was in our reliance on Commercial Off the Shelf (COTS) technology and open standards. This does not mean that this preference for COTS and open standards is necessarily bad. Cost of military development in both time and money drove the DoD away from military unique solutions. In fact, without COTS and open standard solutions we would not be as technologically advanced as we are in Information Technology (IT) and we would have minimal chance of keeping our allies even remotely interoperable. However, by buying into commercial solutions, our technical vulnerabilities are a proverbial open book. This means that as we grow and develop our IT we will be perpetually looking for holes in proprietary commercial hardware and software that an enemy will exploit. Additionally, we will usually have to wait for the commercial world to develop solutions to plug the holes that are discovered.

---

[19] Adm James Ellis, quoted in Elaine M. Grossman, "U.S. Commander in Kosovo Sees Low-Tech Threats to High-Tech Warfare," Inside the Pentagon, (9 Sep 1999):1.

Now, the skeleton that supports the networks as they exist today are the communications pipes that interconnect all the nodes where the sensor, shooters and decision-makers operate. While some NCW proponents would argue that "carefully designed and skillfully operated"[20] networks are inherently robust meshes or webs with multiple paths and alternate routes, our current and near term deployed telecommunications architectures tend to look more like rural street maps connected by a handful of thin, two-lane highways to fixed site reach-back facilities. It is only CONUS based forces and these fixed reach-back facilities that enjoy membership on the robust worldwide telecommunications infrastructure. Communicators everywhere else do the best they can to keep information flowing along the deployed communications rural routes using a handful of expensive satellite and microwave radio systems. Additionally, the thin reach-back paths are so limited in size that the average U.S. Navy ship at sea has less communications bandwidth than the average home broadband Internet service subscriber. This will change over time but not without an investment in infrastructure such as more satellites or satellite alternatives. The Wall Street Journal quoted a Defense Science Board report as stating that: "All Defense Department-owned communication acquisitions over the next 10 years will not come close to meeting bandwidth requirements."[21] This infrastructure shortfall is both a vulnerability an enemy can exploit and a direct impediment to reaching the NCW vision.

The next technological hazard to today's push toward NCW is security. Besides being a technological issue, it is also a procedural one. The problem is one that Harknett calls the "Access/Security Tradeoff". In the nutshell, the problem is to procedurally determine who needs what information in order to become information enabled while technically limiting the information from access by personnel who might otherwise misuse, abuse, or lose friendly information. A case in point is the classified Secure Internet Protocol Router Network (SIPRNET). Though physical security and user accounts protect SIPRNET

---

[20] Cebrowski, 5.
[21] "Military Feels Bandwidth Squeeze as the Satellite Industry Sputters," The Wall Street Journal, (April 10, 2002):1.

data from access by non-cleared users, SIPRNET completely disregards the second tenet of operational security -- the so called "need to know". Though technological solutions like "firewalls" and passwords help mitigate security issues, they also restrict the flow of information and could undo some of the desirable sharing effects of network-centricity.[22] Another security issue has to do with the proliferation of data to include such things as the Common Operational Picture (COP). For example, the U.S. Marine Corps program called the Digital Automated Communications Terminal (DACT) is intended to give small unit leaders a COP and digital communications capability on a small hand held computer. Unfortunately, the COP in a lot of small unit leaders' hands could lead to the following scenario:

> The platoon commander has his trusty DACT that shows exactly where all of the friendly forces are in near real time and the best guesses as to where the enemy forces are. Somehow, that DACT falls into enemy hands before its data is flushed and/or it is pulled out of the network that keeps it updated. The enemy presumably knows exactly where he is, he also now knows exactly where a whole bunch of friendly forces are … BANG! … the good guys are dead. Is the COP in the platoon commander's hand worth the risk?

Granted, there are technological solutions that would help mitigate this risk but the point is that a little bit of stored data can convey a whole lot of dangerous information if it falls in the wrong hands. Further, since the COP is near real time, target quality data, loss of control of it would be far worse than the loss of an ordinary map and overlay.

Besides the technological pitfalls of NCW, there are also operational planning landmines to avoid. If NCW eventually allows us to flatten our force somewhat because we can better exchange C4ISR information, one area that we probably cannot reduce substantially will be operational logistics. Until we can electronically transmit our beans, bullets and Band-Aids, the operational level of war is safe from extinction. However, as NCW efforts push us to distribute our forces into highly dispersed forward areas, our logistical lines of communication become more and more fragile. Any disruption to the network based on its technological frailties could have catastrophic effects on the logistics support for these dispersed forces. A relatively minor disruption by today standards could generate a deadly delay in re-

[22] Harknett.131-132.

supply or evacuation. The best way to mitigate this risk is through operational logistics planning to cover those instances where the network is not there when you need it. Another operational planning pitfall has been referred to as "loss of resiliency" and relates to force planning. The idea behind the loss of force resiliency is that distributed small forces lack the comeback capability when they are faced with unexpected setbacks. Whereas a nearby unit in reserve can reinforce a unit that is falling back in the face of a superior enemy force, reinforcing a NCW unit may be substantially harder.[23] Operational force planning and logistics planning to move those forces on demand are required to mitigate this type of risk.

The third NCW hazard area involves human factors and leadership. These are perhaps the most complex of the NCW issues because they involve humans in combat interacting with the network. In the future weapons operators might routinely receive automated digital target information from voiceless, faceless and nameless, second hand sources. One of the challenges will be in developing an appropriate level of trust in the combined sensor, shooter and C2 network to facilitate timely engagement.[24] In order to be effective, the network must provide relative certainty that the sensor identified target is an enemy force vice a friendly force and is military rather than civilian. Without this human trust, we will remain in a paralytic state such as in Kosovo when counter battery radars could identify an enemy artillery battery and relay target coordinates to the Combined Air Operations Center (CAOC) in two minutes yet it took another three hours to engage the target. This delay gave the enemy battery time to displace and was due to the requirement for positive identification of the target and verification that it was clear of civilians -- there was both a lack of trust in the network and overarching collateral damage concerns that prevented the use of the information available.[25]

Looking externally, there are certain NCW benefits that our potential adversaries enjoy that we do not, the first is in regard to organizational structure. Given that the DoD was created within in a hierarchical

---

[23] Harknett,134.
[24] MCDP-6, 73.

structured society, it is not surprising that our military maintains a hierarchical structure. A hierarchical structure is also inherent in having a young all volunteer force since our training and progression generates a tiered hierarchy. As members learn more they take on more responsibility and move up the hierarchy. Though the DoD can always be tweaked to remove obsoleteness and trim excess, it will likely remain very hierarchical. With NCW, we are now planning to overlay information network architectures on this hierarchical structure. Though this is not necessarily bad, if one looks at some of our potential adversaries such as the Al Qaeda terrorist organization, it is apparent that they are both networked in structure as well as technology. Their technology may not be as advanced as ours but they also are not burdened with a rigid chain of command, law, regulations, uniforms and all those things that make a professional military legitimate and capable of enforcing their nation's will.[26] This networked structure allows them to operate in a true distributed leadership network that our hierarchical structure tends to oppose. Another advantage that non-state actors such as Al Qaeda have is that they can blend into society and take advantage of domestic infrastructure to keep their information networks active. When a state sponsors their activities, such an in Afghanistan, the U.S. has recourse against the state. While they migrate uninvited around Europe, Asia and Africa we do not have recourse because actions which would otherwise be legitimate Information Warfare (IW) by us against an enemy would now be considered as our use of international IW terrorism against the nations where the terrorists hide.[27]

Planning to Avoid the Mines

The past two sections have discussed some of the drawbacks or pitfalls of NCW as it is being applied today. However, the NCW end-state vision is a promising one if only we can avoid stepping on too many mines along the way. The key to success in NCW is in making the most of its advantages while

---

[25] Bruce R. Nardulli, et al., Disjointed War: Military Operations in Kosovo, 1999, (Santa Monica, CA: RAND 2002), 91.
[26] John Arquilla and David Ronfeldt, Networks and Netwars, (Santa Monica, CA:Rand, 2001), 9
[27] Thomas P. M. Barnett, "The Seven Deadly Sins of Network Centric Warfare", U.S. Naval Institute Proceedings, (January 1999): 3.

minimizing risk. This section will present some guidelines for dealing with the strengths and weaknesses in today's NCW. A good starting point for information planning is the Multi-service Procedures for Joint Task Force-Information Management (JTF-IM). JTF-IM defines terms, discusses IM roles responsibilities and most importantly distributes the responsibility across the JTF staff. All subject matter experts have a role and an obligation to make sure their information is distributed, received and understood by their intended audience and that they in turn receive all of the information they need to perform their staff function in support of the JTF Commander.[28] Where JTF-IM falls short is that it focuses more on information internal to the staff and to/from adjacent staffs and not on the distributed knowledge in depth across the battlespace that NCW would require. The below list of planning guidelines is intended to bridge the gap and avoid the pitfalls previously discussed:

1. **Commander's Intent and Rules of Engagement are the most important messages.**
2. **Impart knowledge vice data.**
3. **Exercise operational subject matter experts.**
4. **Spread knowledge of the enemy but protect knowledge of friendly forces.**
5. **Except in crisis, focus attention on things with long range effects.**
6. **Plan for the network to vanish.**
7. **Keep information simple.**
8. **Exchange information efficiently.**
9. **Make information deliverable by means other than the network.**
10. **Build trust by exercising network-centric ops.**

Commander's Intent and ROE: Although it is getting easier to empower a commander with information "all of the information in the world is useless unless it contributes to effective decision making in battle".[29] To truly empower a commander to act independently, he must also be given

[28] Air Land Sea Application Center (ALSA). Joint Task Force-Information Management (JTF-IM). April, 1999. (also known as FM-101-4, MCRP 6-23A, NWP 3-13.1.16 and AFTTP(I) 3-2.22.).
[29] VanRiper. 5.

authority to act. This authority comes in the form of the higher headquarters commander's intent and Rules of Engagement (ROE). Without freedom to act a commander may be information enabled but operationally hobbled. For this reason, commander's intent and ROE are the most important pieces of information to be exchanged for NCW to work. The intent and ROE give subordinates the starting points for developing their plans of action against the enemy. Without them subordinates must "check with the boss first" and the network becomes a long leash instead of a tool of empowerment and synchronization.

Impart knowledge vice data: Knowledge is information that has been processed by humans to have meaning and value based on intuition and experienced judgment.[30] Data can be overwhelming and requires reprocessing by each recipient. Data that a JTF staff processes and distributes as knowledge requires no reprocessing, can clarify commander's intent based on a changing situation and puts all receiving subordinates on the same sheet of music where they know what the commander knows and believes. One of the operational staff's jobs is to analyze the broad operational situation and synthesize it into a product on which subordinates can act. In doing this, they relieve subordinate commanders of having to do it all for themselves and allow their subordinates to focus attention on the enemy in and around their area of responsibility. Distribution of situational knowledge based on the commander and staff's intuition and judgment is essential to successful NCW.

Exercise operational subject matter experts: This means not only exercising them in their area of expertise but also having them develop their information exchange requirements and mechanisms. Knowing what to know is a key element for successful NCW.[31] Fortunately, on operational staffs we have subject matter experts that know exactly what they need to know. They also possess experience that their subordinate staff counterparts lack. These experts must not only be kept in the loop as NCW operations begin to pick up tempo and lean toward self-synchronization, they also must be dragged,

---

[30] VanRiper. 9.
[31] Commander Alan D. Zimm, USN (Ret.), "Human-Centric Warfare," U.S. Naval Institute Proceedings (May 1999):29-30.

kicking and screaming if necessary, into the NCW information exchange planning process. Each member of a JTF staff is responsible for their own information. The Information Management Officer (IMO) will coordinate the effort and the staff J-6 can provide some technical guidance but J-6 staffs are more correctly viewed as electron managers rather than information managers.

Spread knowledge of the enemy but protect knowledge of friendly forces: This is perhaps one of the weakest links in the current implementations of NCW. Intelligence products are often highly classified or compartmentalized and do not move around the battlefield easily. However, with initiatives such as that of the Director of Central Intelligence to get the intelligence community to use more and more commercial satellite imagery resources, that trend may be changing.[32] In general, any knowledge of the enemy that does not involve divulging sources and methods of collection is a good thing. As more and more of these commercial resources become available, we may come to a time when a force can enter a city with a commercial aerial photo in the hands of every squad leader to help him navigate. An interesting example of the networked sharing of knowledge about the enemy is the international crime information clearing-house called Interpol. Though Interpol has no authority to direct action or enforce law in its participating countries, it serves as a tremendous information exchange network in the continuous worldwide fight against crime.[33]

On the flip side of spreading information about the enemy is protecting the friendly information. NCW planning must include developing means to parse out and segregate the COP data and other relevant information about a unit's combat area so that few if any other unit locations, missions and dispositions are compromised if one unit loses their computer based decision aids. Though we would certainly desire commanders to have enough of the COP to coordinate with adjacent units and distinguish friend from foe, only a small portion of the JTF COP would be required to do that. Controlling the flow

[32] Glen W. Goodman. "Unclassified Space Eyes," The ISR Journal, (2002/Issue 4):24.
[33] Interpol. "Interpol-An Overview", Interpol HQ, Lyon, Fr.,4.

to only that minimal amount of friendly information that is required will also help mitigate the hazards of "macro-management" discussed earlier.

Except in crisis, focus attention on things with long range effects: In order to be effective, JTF staffs must think long-term and look down range. Operational success stems from planning an operation with all its incumbent parts while looking toward future follow on operations. A popular self-help guru, Stephen Covey, would refer to this as staying within the "Quadrant of Quality". Covey has a quaint little model to help people stay focused on tasks that will help them succeed in life. This model has four quadrants: I) Important/Urgent, II) Important/Not Urgent, III) Not-Important/Urgent, IV) Not-Important/Not-Urgent.[34] For a JTF Quadrant II is also the "Quality Quadrant" as it is the quadrant where all long range planning, analysis and intuitive thinking reside. JTF Commanders and their staffs need to make a conscientious effort to stay away from Quadrants II and IV where the mundane "not important" tasks reside no matter how compelling it is to watch the COP or dabble in the details particularly, those details that belong to the tactical level of war. JTF staffs must plan their information distribution so that they can remain focused on the future and shaping the battle. Proper planning will help to prevent the NCW hazard of "micro-management".

Plan for the network to vanish: Due to the nature of the combat environment and the relatively light distribution of communications equipment suites capable of transporting large amounts of network data, JTF staffs must plan that they will fail or be dramatically degraded at various times. Though there are lots of telephones and man-pack radios in the operational environment today, telephone circuits outside a Command Post (CP) mostly traverse the same communication pipes as the network data. Further radios are generally not capable of transporting data to the degree which users are beginning to get accustomed. JTF staffs also need to be aware that communications pipe outages tend to take out all network services

[34] Stephen R. Covey, A. Roger Merrill and Rebecca R. Merrill, First Things First: to live, to love, to learn, to leave a legacy, (New York: Simon & Schuster, 1994), 37.

so e-mail, web browsing and COP transfer can all disappear simultaneously. The point here is to make sure that each section of the JTF staff is prepared to conduct critical business via non-network means. Better yet, the JTF can plan to always operate in a manner that decreases the reliance on the network. The idea is to take advantage of the network but to never become dependent on it. With this approach, the NCW force can continue to fully operate for an extended period without network connectivity.

Keep information simple, exchange information efficiently, and make information deliverable by means other than the network: These three guidelines are grouped together because they all relate to making the most of the limited tactical communications bandwidth available. Keeping information simple tends to minimize the total amount of data transmitted. Exchanging it efficiently deals with packaging the information so that it is smaller for transport. Most everyone is familiar with "zipping" files but there are other less obvious methods for reducing the size of the information package. For example, transferring images and maps consumes a lot of bandwidth compared to overlays so if the staff only sends a map once and changes overlays frequently there will be a tremendous savings. Conscientious media selection is also critical. Given that a single Video Tele-Conference (VTC) can consume a large percentage of total available network sources and can block dozens of telephone circuits to other commands for its entire duration, the cost of using a service must always be weighed. For example, using VTC to share a Power Point briefing not only does not usually work very well, it could feasibly cost ten times the bandwidth as e-mailing the file and conducting a voice tele-conference. JTF staff members do not need to become communications experts to exchange information efficiently since they have a J-6 to consult. However, the staff does need to be aware of relative costs of media types and plan to use only the minimal amount of information exchange necessary to convey their message. Making information deliverable by other than network means involves packaging it up on removable media (disk, CD, paper, etc.). This can be used to mitigate the risks of outages but it can also be used to

distribute large amounts of fixed information in advance of an operation so that only updates and changes needed to be transferred via the busy network once the operation begins.

Build trust by exercising network-centric ops: For a variety of reasons previously discussed, trust is something that is lacking in our networks today. Part of this lack of trust is based on the fact that our sensors are not yet good enough to guarantee that the icon on the screen is indeed enemy rather than friendly and military instead of civilian. Technology may change this but once it does, the human part of the trust equation will need to be developed. The only way to build this human trust to the degree required for the distributed, self-synchronized combat operations called for by NCW is to develop integrated network information planning and to practice. In order for commanders to be confident that the information they are being fed via the network is correct, they need to be fully cognizant of and comfortable with the information exchange mechanisms built into the network. They will want to know what checks and balances have been built in to the system to help them prevent fratricide or avoidable collateral damage. Once they have faith in what the network is telling them, they will be better able to act.

Conclusion

MCDP-6 begins with an account of a modern information enabled force in a fictitious operation called VERBAL IMAGE. In one part of the operation, a battalion commander is busily watching the COP and redirects a platoon commander in one of his subordinate companies to maneuver through an area that is blocked with dense vegetation. Only the platoon commander on the scene could see what the terrain actually looked like and that it was impassable. Elsewhere, an attack helicopter pilot comes across an unexpected enemy force and lands to reorient a rifle company towards the new objective. Clearly the

second scenario is what we desire out of NCW while the first scenario illustrates what we endeavor to avoid. Superior information may give us some operational advantages over our adversaries but the information is only valuable if it is correct, timely, accurate and if we are empowered to act on the information. Additionally we must have as much trust in the information as if our immediate superior commander were saying it to our face. Warfare is complex, dangerous and full of confusion. The planning guidance offered above is intended to help JTF staffs wrestle with the issues affecting NCW operations before they become untenable. Through practice in network-centric environments and improvements in technology and resources, we will hopefully achieve the vision of NCW while mitigating all of its risks through action or tactics techniques and procedures.

Bibliography

Air Land Sea Application Center (ALSA). Joint Task Force-Information Management (JTF-IM). April, 1999.

Alberts, David S., John J. Garstka and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP Publication Series, 1999.

Arquilla, John, and David Ronfeldt. Networks and Netwars. Santa Monica, CA: RAND, 2001.

Barnett, Thomas P. M. "The Seven Deadly Sins of Network-Centric Warfare." U.S. Naval Institute Proceedings 125, no. 1(January 1999):27-45.

Britten, Scott M. "Directing the War from Home." The Technological Arsenal: Emerging Defense Capabilities. Washington D.C.: Smithsonian Institute Press. 2001: 199-219

Cebrowski, Arthur K. and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." U.S. Naval Institute Proceedings (Jan 1998): 28-35.

Cebrowski, Arthur K. "Network-Centric Warfare: An Emerging Response to the Information Age." Lecture. U.S. Naval War College, Newport, RI: 29 June 1999.

Covey, Stephen R., A. Roger Merrill and Rebecca R. Merrill. First Things First: to live, to love, to learn, to leave a legacy. New York: Simon & Schuster, 1994.

Dahl, Erik J. Network Centric Warfare and the Death of Operational Art (NWC 1012). U.S. Naval War College, Newport, RI.

Ellis, James O. "A View from the Top." Allied Force After Action Briefing, n.d.

Goodman Jr., Glenn W. "Unclassified Space Eyes." The ISR Journal (2002/Issue 4): 24-35.

_____. "More Than Just Platforms & Sensors." The ISR Journal (2002/Issue 1): 26-29.

Grossman, Elaine M. "U.S. Commander in Kosovo Sees Low-Tech Threats to High-Tech Warfare". Inside the Pentagon (9 Sep 1999):1.

Hammes, T.X. "War Isn't a Rational Business." U.S. Naval Institute Proceedings (July 1998): 22-25.

Harknett, Richard J. and the JCISS Study Group. "The Risks of a Networked Military." Orbis, (Winter 2000):127-143.

Interpol. Interpol: An Overview. Lyon, France, n.d. http://www.interpol.com/Public/ICPO/InterpolOverview.pdf

"Military Feels Bandwidth Squeeze as the Satellite Industry Sputters." The Wall Street Journal, (10 April 2001):1.

Nardulli, Bruce R. et al. Disjointed Warfare: Military Operations in Kosovo, 1999. Santa Monica, CA: RAND, 2002.

Owens, William A. “An Emerging Syatem of Systems.” U.S. Naval Institute Proceedings (May 1995):35-39.

Shattuck, Lawrence G. “Communicating Intent and Imparting Presence.” Military Review. Fort Leavenworth, KS.: U.S. Army CGSC.

Smith, Edward A. “Network-Centric Warfare: What’s the Point?” Naval War College Review. (Winter 2001): 59-75.

U.S. Marine Corps. MCDP-6 Command and Control, Washington: Headquarters, U.S. Marine Corps, 4 Oct 1996.

Van Riper, Paul K. “Information Superiority,” U.S. Congress, House, Procurement Subcommittee and Research and Development Subcommittee, 20 March 1997.

Zimm, Alan D. “Human-Centric Warfare” U.S. Naval Institute Proceedings (May 1999): 28-31.